## What is claimed is:

**[Claim 1]** 1. A computer program, embodied on a computer readable storage medium, for assisting a user to determine whether an email comes from a purported originator, the computer program comprising:

a code segment that determines with a computerized system whether the email includes an authenticity mark including an originator identifier and encrypted data;
a code segment that decrypts said encrypted data based on said originator identifier, into decrypted data;
a code segment that presents to the user on a display unit:
whether the email includes said authenticity mark;
whether said encrypted data decrypts successfully; and
information based on said authenticity mark and said decrypted data.

**[Claim 2]** 2. The computer program of claim 1, wherein the computer program is digitally signed.

**[Claim 3]** 3. The computer program of claim 1, wherein said code segment that determines runs as a service in said computerized system.

**[Claim 4]** 4. The computer program of claim 1, wherein said code segment that determines includes a hypertext transport protocol (HTTP) server.

**[Claim 5]** 5. The computer program of claim 1, wherein said code segment that determines listens at a port in said computerized system for a request for hypertext markup language (HTML) content and extracts said authenticity mark from a uniform resource locator (URL) link requesting said HTML content.

**[Claim 6]** 6. The computer program of claim 1, wherein said code segment that presents further presents information to the user based on said originator identifier.

**[Claim 7]** 7. The computer program of claim 6, further comprising a code segment that matches said originator identifier to one of a plurality of registered originators maintained in a storage unit, to retrieve a decryption

key associated with said originator identifier for use by said code segment that decrypts.

**[Claim 8]** 8. The computer program of claim 1, wherein:

said code segment that determines compares a checksum from said authenticity mark against contents of the email; and
said code segment that presents further presents to the user information based on said checksum.

**[Claim 9]** 9. The computer program of claim 1, wherein said code segment that decrypts employs a public key of said purported originator.

**[Claim 10]** 10. The computer program of claim 1, wherein:

said code segment that decrypts extracts at least one of a timestamp, a topic, and a user identifier from said encrypted data; and
said code segment that presents further presents to the user information based on at least one of said timestamp, said topic, and said user identifier.

**[Claim 11]** 11. The computer program of claim 10, further comprising a code segment that compares said timestamp to preset timeliness criteria; and wherein said code segment that presents emphasizes said information based on said timestamp when said timeliness criteria are deviated from.

**[Claim 12]** 12. The computer program of claim 1, wherein said code segment that presents employs a dialog box that only software running locally in said computerized system can provide, thereby avoiding confusion with a remotely generated browser window.

**[Claim 13]** 13. A system for assisting a user to determine whether an email comes from a purported originator, the system comprising:

a computerized system having a display unit;
a logic in said computerized system that determines whether the email includes an authenticity mark including an originator identifier and encrypted data;
a logic in said computerized system that decrypts said encrypted data based on said originator identifier, into decrypted data;
a logic in said computerized system that that presents to the user, on said display:

whether the email includes said authenticity mark;
whether said encrypted data decrypts successfully; and
information based on said authenticity mark and said decrypted data.

**[Claim 14]** 14. The system of claim 13, wherein said logic in said computerized system that determines runs as a service.

**[Claim 15]** 15. The system of claim 13, wherein logic in said computerized system that determines includes a hypertext transport protocol (HTTP) server.

**[Claim 16]** 16. The system of claim 13, wherein said logic in said computerized system that determines listens at a port for a request for hypertext markup language (HTML) content and extracts said authenticity mark from a uniform resource locator (URL) link requesting said HTML content.

**[Claim 17]** 17. The system of claim 13, wherein said logic in said computerized system that that presents to the user further presents information based on said originator identifier.

**[Claim 18]** 18. The system of claim 17, further comprising a logic in said computerized system that matches said originator identifier to one of a plurality of registered originators maintained in a storage unit, to retrieve a decryption key associated with said originator identifier for use by said logic in said computerized system that decrypts.

**[Claim 19]** 19. The system of claim 13, wherein:

said logic in said computerized system that determines compares a checksum from said authenticity mark against contents of the email; and
said logic in said computerized system that that presents to the user further presents information based on said checksum.

**[Claim 20]** 20. The system of claim 13, wherein said logic in said computerized system that decrypts employs a public key of said purported originator.

**[Claim 21]** 21. The system of claim 13, wherein:

said logic in said computerized system that decrypts extracts at least one of a timestamp, a topic, and a user identifier from said encrypted data; and
said logic in said computerized system that that presents to the user further presents information based on at least one of said timestamp, said topic, and said user identifier.

**[Claim 22]** 22. The system of claim 13, further comprising a logic in said computerized system that compares said timestamp to preset timeliness criteria; and wherein said logic in said computerized system that that presents to the user emphasizes said information based on said timestamp when said timeliness criteria are deviated from.

**[Claim 23]** 23. The system of claim 13, wherein said logic in said computerized system that that presents to the user employs a dialog box that only software running locally in said computerized system can provide, thereby avoiding confusion with a remotely generated browser window.

**[Claim 24]** 24. A method for assisting a user to determine whether an email comes from a purported originator, the method comprising:

determining whether the email includes an authenticity mark including an originator identifier and encrypted data;
decrypting said encrypted data based on said originator identifier, into decrypted data;
presenting to the user:
whether the email includes said authenticity mark;
whether said encrypted data decrypts successfully; and
information based on said authenticity mark and said decrypted data.

**[Claim 25]** 25. The method of claim 24, wherein said determining includes running a service in a computerized system.

**[Claim 26]** 26. The method of claim 24, wherein said determining includes running a hypertext transport protocol (HTTP) server.

**[Claim 27]** 27. The method of claim 24, wherein said determining includes listening at a port in a computerized system for a request for hypertext

markup language (HTML) content and extracting said authenticity mark from a uniform resource locator (URL) link requesting said HTML content.

**[Claim 28]** 28. The method of claim 24, wherein:

said determining further includes extracting an originator identifier from said authenticity mark; and
said presenting further includes presenting information to the user based on said originator identifier.

**[Claim 29]** 29. The method of claim 28, further comprising matching said originator identifier to one of a plurality of registered originators and retrieving a decryption key associated with said originator identifier for use in said decrypting.

**[Claim 30]** 30. The method of claim 24, wherein:

said determining includes comparing a checksum from said authenticity mark against contents of the email; and
said presenting includes presenting information based on said checksum.

**[Claim 31]** 31. The method of claim 24, wherein said decrypting employs a public key of said purported originator.

**[Claim 32]** 32. The method of claim 24, wherein:

said decrypting extracts at least one of a timestamp, a topic, and a user identifier from said encrypted data; and
said presenting includes presenting information based on at least one of said timestamp, said topic, and said user identifier.

**[Claim 33]** 33. The method of claim 32, further comprising comparing said timestamp to preset timeliness criteria; and wherein said presenting emphasizes said information based on said timestamp when said timeliness criteria are deviated from.

**[Claim 34]** 34. The method of claim 24, wherein said presenting employs a dialog box that only software running locally in a computerized system can provide, thereby avoiding confusion with a remotely generated browser window.